Identity Based Secure Routing For Wireless Ad-Hoc Networks

Deepak Kumar Sharma[1], Dr. S. K. Saxena[2], Yogesh Sharma[3], Ajay Tiwari[4]
[1] Maharaja Agrasen Institute of Technology, Computer Science Department, Delhi, India, dk.sharma1982@yahoo.com
[2] Delhi College of Engineering, Department of Computer Engineering, Delhi, India, saxena_58@yahoo.com
[3]Maharaja Agrasen Institute of Technology, Computer Science Department, Delhi, India, yogesh027@yahoo.co.in
[4] Maharaja Agrasen Institute of Technology, Computer Science Department, Delhi, India, ajaytiwari04@gmail.com

Abstract— **In this paper, we propose an Identity (ID)-based Secure Routing Scheme for secure routing in wireless ad-hoc networks. It make use of Identity based Signature scheme and hash chains to secure the AODV (Ad-hoc on demand distance vector routing) messages. We have used ID based Signature scheme for the immutable fields, that is the fields that remain same throughout the journey of the routing packet and Hash Chains for the mutable fields (fields which changes from node to node) e.g. Hop Count. This system has the following advantages as compared to the previous solutions, most of which uses RSA based Public Key Cryptographic solutions. Firstly, it makes use of Identity based signature scheme which is certificateless thus saving overhead costs of communication and storage. Secondly, in ID based schemes we can use our identity, like our IP address or email ID as our public key, which leads to smaller key size as compared to other cryptographic techniques. Also this system does not require establishment of any third party like PKI (Public-key Infrastructure) at the initial stages of network establishment**

Index Terms— **Security, Wireless Ad-hoc Networks, Routing Protocols, ID-based Cryptography, Secure AODV.**

I. Introduction

A Mobile Ad hoc Network, or MANET, consists of a group of cooperating wireless mobile hosts (nodes) that dynamically constructs a short lived and self-configuring network without the support of a centralized network infrastructure. The mobile nodes can be cell-phones, PDAs and laptops and typically support wireless connectivity like 802.11, Bluetooth, etc. MANETs are fundamentally different from their wired-side counterparts. They provide no fixed infrastructure, base stations or switching centers. Moreover, the nodes of a MANET are computationally constrained and have limited power.

Routing is an important function in any network, be it wired or wireless. The protocols designed for routing in these two types of networks, however, have completely different characteristics. Routing protocols for wired networks typically do not need to handle mobility of nodes within the system. These protocols also do not have to be designed so as to minimize the communication overhead, since wired networks typically have high bandwidths. Very importantly, the routing protocols in wire line networks can be assumed to execute on trusted entities, namely the routers.

These characteristics change completely when considering ad hoc wireless networks. Mobility is a basic feature in such networks. Resource constraints like limited bandwidth and computing power of the devices also aggravates the problem of designing routing protocols for such networks which do not require high bandwidths. Ad hoc networks also do not have trusted entities such as routers, since every node in the network is expected to participate in the routing function. Therefore, routing protocols need to be specifically designed for wireless ad hoc networks.

Ad-hoc routing protocols, including AODV (Ad-Hoc Distance Vector Routing) [1], DSR (Dynamic Source Routing)[15], OLSR (Optimized Link State Routing), etc are designed for performance, not security, and thus all of them are subjected to some kind of attacks. These attacks include, packet dropping, modification of packets (modifying sequence numbers, hop count, etc), impersonation, replaying of old routing information etc. These attacks can partition a network or may introduce excessive load into the network by causing retransmission and inefficient routing.

The Ad hoc On Demand Distance Vector (AODV) [1] [7] routing algorithm is a reactive routing protocol designed for ad hoc mobile networks. To transmit data over an ad-hoc network, the AODV protocol enables dynamic, self-starting, multi-hop routing between mobile devices. It allows these mobile computers, or nodes, to pass messages through their neighbors to nodes with which they cannot directly communicate.

In this paper we have tried to integrate the concept of Identity Based Signature Generation Schemes instead of traditional signature schemes to AODV so as to secure the routing process without incurring much overhead on the system. This signature scheme will allow us to use Email-ID and IP address as our public key, thus eliminating the need of any certificates which will save the network bandwidth. Also ID based signature schemes are based on Pairing based

DOI: 01.ijns.01.02.05

cryptography which allows us to use smaller key size maintaining a similar of security as provided by other schemes.

II. Background And Related Work

Currently, some solutions propose to use cryptographic methods to secure the ad-hoc routing protocols. Those methods include, HMAC (Hashed Message Authentication Code)-based schemes, such as SRP [5], digital-signature-based scheme, such as SAODV [7] (for AODV) and ARAN [4] (for DSR), and hash-chain-based or TESLA-based [4] scheme, such as SEAD [4] (for DSDV) and Ariadne [16] (for DSR) and identity based secure routing. However, HMAC-based schemes provide only peer-to-peer message authentication, not broadcast message authentication, so they are not suitable for broadcasting-based routing messages. Digital-signature-based schemes (like SAODV) can achieve broadcast message authentication, but all these schemes need the certificate, which incurs a large amount overhead in communication, computation and storage. TESLA based schemes use the time synchronization to avoid such a problem, but it may not be practicable for general applications. The Identity based routing framework [8], [14] solves most of these problems and even reduces the key size drastically. Also the problem of key distribution is minimized as the Identity of the user serves as its public key. But it requires signing and verifying the message at each node, which requires high computation, and devices that take part in the ad-hoc network are battery operated on which this computation of signature generation and verifying can be battery consuming and thus can degrade the network performance.

The rest of the paper is organized as follows. Section III presents our proposed scheme, and Section IV describes the integration of Signature scheme in AODV, Section V presents an analysis on security and performance, Section VI presents Results And Evaluation and Section VII concludes the paper.

III. Proposed Scheme

A. Design Rationale

Until now signature based authentication scheme made use of certificates and CRL (Certificate Revocation List) both requiring high storage and communication costs. Traditional certificate-based public key algorithms require digital certificates to authenticate the public key. A digital certificate is a data structure that contains the public key itself and the signature of the public key signed by a trusted 3rd Party. The management of certificates is nontrivial in ad-hoc networks. The storage of the certificates in not negligible and their transportation increases the load of the network. Further if the private key is stolen the certificates have to be revoked and the network has to be alerted of it.

This problem was solved by the Identity based Signature Scheme, which is a public key encryption scheme, in which any string with which users can be commonly identified is used as their public key for instance their ID or Email Id. The corresponding private key is generated by a trusted 3rd party, called PKG and kept secret by the owner of the ID. The authentication of public key is not required because nobody else than the owner of the ID can have the private key. This eliminates to transmit or store digital certificates and also lowers the key size.

So we propose that the Identity based Signature scheme be applied to the message at the source node on the authentication of immutable fields in the packet header, while the mutable fields should be protected by the hash chain. Thus this scheme can efficiently protect both types of fields in the packets. As of now many ID based encryption scheme have been proposed, but in this paper we propose to use the BLMQ [11] signature scheme as it reduces the number of pairing operations required in the verification and signature process. The signature generation and verification process using BLMQ has been explained below.

B. BLMQ – ID-Based Signature Scheme

The rationale behind ID based signature scheme is the bilinear pairing which has some wonderful properties as the building block for public key cryptosystem. Let G1 be an additive group of prime order q and G2 be a multiplicative group of the same order. Let P denote a generator of G1. The Discrete Logarithm Problem (DLP) in these groups in believed to be hard. A bilinear pairing is a map e: $G1 \times G1 \rightarrow G2$ with the following properties:

1. Bilinear: e (aQ1, bQ2) = e (bQ1, aQ2) = e (P,Q)ab where Q1, Q2 ∈ G1 and a, b ∈ Zq*.
2. Non-degenerate: e (P, P) ≠ 1and therefore it is a generator of G2.
3. Computable: There is an efficient algorithm to compute e (Q1, Q2) for all Q1 Q2 ∈ G1.

G1 will be the group of points on an elliptic curve and G2 will be a multiplicative extension of a finite field. The map e will be derived from either the Weil pairing or Tate pairing on an elliptic curve of a finite field. However the Tate pairing is considered twice as fast as Weil pairing [5]. An ID Based Signature generation scheme consist of four main steps. With respect to these steps, the BLMQ Scheme can be explained as:-

B1. Setup

1. Select a security parameter k. For the implementation k ≈ m, the field length.
2. Select a k bit prime number l , and bilinear map groups (G1,G2,GT) of order supporting

DOI: 01.ijns.01.02.05

an efficiently computable, non-degenerate pairing e : G1× G2 → GT. In this case G1 = G2 = E(F2m), that is the Elliptical Curve Group defined over binary field, and GT = F*q k , that is the multiplicative group of the extension field. l is the order of the groups G1 , G2.

3. Select Generators (l torsion points)P ∈ G1, Q ∈ G2, P and Q here are any points on the elliptic curve, since the order of the curve $l = \#E_b$ has been chosen and it is known that there are , torsion points on a curve therefore in our case any point selected on the curve will be its generator.
4. Hash functions h0 : GT × {0 1}*→ , h1 : {0 1}*→ Z_l^* . denotes the multiplicative groups of the prime number l. The Hash functions H0 and H1 can be implemented using the normal cryptographic Hash functions like SHA, thus avoiding any use of point to map Hash Functions.
5. A master key s→Z_l^* is chosen, with which the public key Ppub = sP ∈ G1 is associated. This part of the algorithm make use of Elliptic Curve Arithmetic for calculating the system public key Ppub.
6. The generator g = e(P, Q) ∈ GT , g ∈ GT (element of extension field) is the result of applying the pairing algorithm on the selected points P and Q.
7. Thus the public Parameters are :

k, l , G1,G2,GT , P, Q, g, Ppub, e, h0, h1

But since the Elliptical Groups and the Hash Functions are already there with each of the participating nodes, the parameters that actually need to be transmitted are:-

k, P, Q, g, Ppub ,

B2. Private-Key Extraction

This part of algorithm deals with the allocation of Private key to a node, once the node submits its identity. Following steps are taken:

1. The Private Key Generator, PKG takes as input entity A's identifier IDA ∈ {0, 1}* and extracts A's identity-based private key QA ← (h1 (IDA) + s) −1 Q ∈ G2. This process requires the support for BigIntegers, a class that can deal with numbers of arbitrary large size and Elliptic Curve Arithmetic for calculating the Private Key QA, which is actually a point on the Curve. This communication takes place using a secure channel and with the help of secure key distribution system, so that only the correct node gets the private key and no node can impersonate some other node. No secure channel has been established it is assumed that one already exist in the network.
2. A node can verify the consistency of his key by checking e(h1(IDA)P + Ppub QA) = g. The above method of key establishment is called Sakai Kasahara key style [Sakaiand Kasahara 2003].

B3. Signature Generation

The process of signing a message m ∈ {0, 1}* under the private key QA, consist of the following steps:

1. The signer picks u ← Z_l^*, that is it selects a random number from the multiplicative group of .
2. It computes r ←g^u. This step requires us to perform exponentiation in the extension field GT.
3. h ← h0(r, m).
4. S ← (u − h)QA. It involves Elliptic curve arithmetic as QA is a point on the curve.

The signed message is the triple

(m, h, S) ∈ {0, 1}* × Z_l^*

Therefore it can be seen that signature is a composition of two main things besides the message. First 'h', which is a number that belongs to Z_l^*, and thus it is approximately a k bit number, since k is large (>= 160 for good security).Second S, it is a point on the elliptic curve and hence requires support for curve arithmetic. Thus it can also be seen that no pairing is involved in the signing process, which makes the signature generation an efficient process.

B4. Signature Verification

This part of the algorithm deals with the verification of the signature (m, h, S), given the public key of the signer IDA. The algorithm performs the following steps.

1. r ← e(h1(IDA)P + Ppub, S) gh
2. v ← h0(r, m)

The verifier accepts the signed message iff v = h.

IV. Integrating the Signature scheme in AODV

The above described signature generation scheme was integrated into the existing AODV code in the NS2 (Network Simulator –2) with the purpose of securing the routing messages, this needs some changes to be made to the existing NS2 AODV implementation. The basic aim is that each node should sign the routing packet it generates using Signature scheme implemented. The IP address of the node has been chosen as its Public Key and the message to be signed here is the Routing Packet. Each intermediate node then first verifies the packet it receives and only then any further processing takes place. The Routing packets mainly consist of two kinds of field:

1. Non-Mutable : Which remains same throughout

DOI: 01.ijns.01.02.05

the journey of the packet.

2. Mutable: Fields whose value can be altered by the intermediate nodes, like Hop Count.

Each node signs only the Non-Mutable fields with its private key, and then forwards the packet after integrating the signature and its public key in it. In this paper only Non-Mutable fields have been dealt with. Existing solutions like Hash Chains can be used for dealing with Mutable fields.

A. Changes made to AODV

The embedding of the signature required the following changes in the existing NS2 implementation of AODV.

1. In the existing implementation of the AODV, the RREP message was modified while forwarding the reply, which prohibited the signing of the message. Some changes were made to the routing process so that there was no need to modify the RREP while forwarding the reply.
2. Route Reply by an intermediate node on behalf of the destination node has been disabled, since the intermediate nodes cannot sign on behalf of the destination node.
3. Packet format was extended to include two more fields,
   i. ID: Public key of the node, who signed the message.
   ii. Signature: It is obtained by applying the Signature Scheme on the Routing Packet (not including the Hop count field).

As the signature is a combination of a (h, S). Thus in the packet also the Signature is represented as a combination of 2 fields.

i. BigInt number , h.
ii. A Point on the Elliptic Curve, S.

Both of these fields were converted into a character array format for embedding them into a packet. Table 1 below shows the extended packet format of AODV.

TABLE 1
EXTENDED PACKET FORMAT OF AODV

RREQ / RREP
ID (Public key of node)
Signature = {RREQ/RREP - HopCount}K-1a

B .Initializing the routing Process

All the nodes first obtain their copy of Public Parameters, from the PKG (Private Key Generator). No special key distribution scheme have been used, the PKG is represented in the library as PKG.{h, cc}. It returns a structure named Public Parameter to the node that requested the parameters; this structure contains all the required public parameters. The Node then submits their Identity (Public Key) to the PKG to obtain the Private Key. This process should be made via a secure channel so that the key is delivered to the correct owner. The establishment of the secure channel has not been considered in this paper.

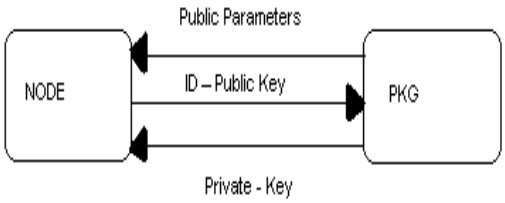

Fig.1 Key Distribution

C. Securing the Routing Process

In this paper emphasis has been made on securing the RREP and RREQ messages. Other routing messages like RRER and HELLO messages can be secured in a similar way.

C1. Sending RREQ/RREP

(i) Before sending the RREQ/RREP packet (which is filled with the required info), the sender signs the packet with its private key. Hop count field (which is a mutable field) is set to zero before signing and then restored again.
(ii) The signing node then inserts its Public Key (ID) and the Signature generated into the Packet.
(iii) Finally the packet is transmitted.

C2. Receiving RREQ/RREP

(i) Any intermediate node receiving the RREQ first verifies the signature of the sending node in the packet.
(ii) If the signature is verified only then any further processing takes place on the packet (like setting up reverse path or sending RREP), else the packet is dropped.

V. Security and Efficiency Analysis

A. Security Analysis

Only authorized node with the right private key issued by PKG can generate qualified routing packets. Without the signature that is generated using private key, the packet will be looked as garbage and dropped by the receiver. The nodes will be re- authenticated when they request the private key. The PKG will be the single failure point and vulnerable to the attacks, however, the distributed PKG and threshold cryptography can be utilized to deal with it. Because the fixed fields in the message are signed by the initiator, any other nodes can not modify it without

DOI: 01.ijns.01.02.05

being detected. Since the mutable field of hop count is being hashed at every step. The non-repudiation of changeable fields can detect the misbehaviors of former nodes and drop the malicious packets intermediately.

B. Efficiency Analysis

At the initiator the major operation is signing and at each intermediate node the major operation is verification. And the pairing is computationally most expensive task involved in this process. However choosing the right parameters for the pairing, like right elliptical curve, field selection, field arithmetic and pairing algorithm used can highly increase the efficiency of the pairing. The best result of pairing reported by [12],[13] is 8.7 ms, with the help of dedicated hardware this can further be improved.

Also the public key size is also very small, 160 bit key provides a security equivalent to that provided by 1024 bits in RSA, and there is no need to include any certificates in the packet which leads to a huge saving in the bandwidth.

VI. Results And Evaluation

For the finite field F2m with m = 163 the following results were obtained by using the clock () function of C++ time.h header file to execute the code for the following operations:

TABLE 2
TIMING RESULTS

Operation	Time (ms)
Pairing	25
Signature Generation	7
Signature Verification	30

Following graphical results were obtained by performing the simulation of AODV integrated with ID-Based Signature Scheme using NS2. The simulation environment consisted of 20 nodes moving over an area of 670 X 670. Three parameters Throughput of sending and receiving packets, sum of number of all packets dropped by using the original AODV and using AODV + ID Based Signature.

A. Throughput of Sending packets

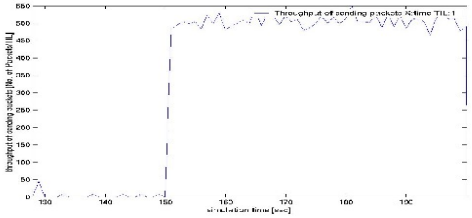

Fig 2. AODV + ID Based Signature

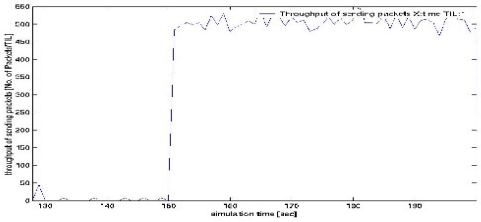

Fig 3. AODV

B. Throughput of Receiving packets

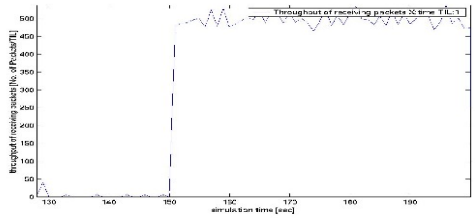

Fig 4. AODV + ID Based Signature

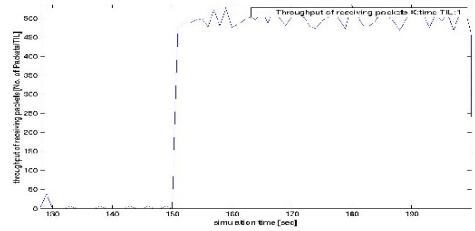

Fig 5. AODV

C. Sum of number of all Packets Dropped

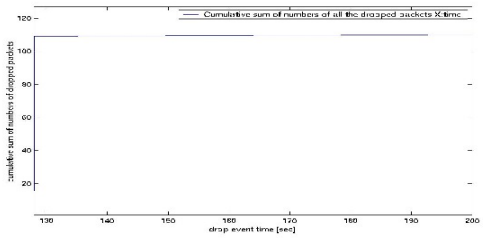

Fig 6. AODV + ID Based Signature

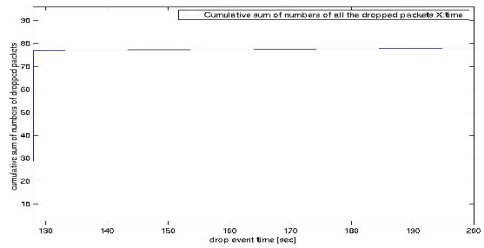

Fig 7. AODV

VII. Conclusions And Future Work

The ID based Signature scheme has been successfully implemented and the same is integrated into the AODV. The timing results for the pairing algorithms and the key generations and verification

DOI: 01.ijns.01.02.05

has been shown. The graphical results for the throughput of the system with signature scheme integrated in AODV have also been shown.

Although the throughput of the system has decreased for normal circumstance but the system has gained the capability to defend itself in the event of any node being malicious. The most important algorithm involved in the signature scheme is the pairing; the efficiency of the pairing algorithm should further be improved to reduce the time required in signature generation and verification.

- Use of dedicated hardware for performing the arithmetic can improve the overall throughput of the system.
- Use of Threshold Cryptography can avoid the key escrow problem associated with ID based system.
- Mixed coordinate system can improve the elliptical curve arithmetic.
- Presently we have secured only the Non-mutable fields, and for complete security and efficient method for securing mutable field in the routing packets should also be employed.

REFERENCES

[1] Luke Klein-Berndt Wireless Communications Technologies Group National Institute of Standards and Technology, "A Quick Guide to AODV Routing".

[2] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," CRYPTO' 84, LNCS, 1985, pp. 53–57.

[3] Joonsang Baek, Jan Newmarch, Reihaneh Safavi-Naini, and Willy Susilo, School of Information Technology and Computer Science, University of Wollongong, "A Survey of Identity-Based Cryptography".

[4] Darrel Hankerson , Alfred Menezes, Scott Vanstone , "Guide to Elliptic Curve Cryptography".

[5] G. Berton, L. Breveglieri, P. Fragneto1, G. Pelosi and L. Sportiello ST Microelectronics1, Politecnico di Milano "Software Implementation of Tate Pairing over GF(2^m)".

[6] Yih-Chun Hu University of California, Berkeley; Adrian Perrig Carnegie Mellon University "A Survey of Secure Wireless Ad- hoc Routing".

[7] C. Perkins, E. B. Royer and S. Das, "Ad-hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, Jul. 2003.

[8] Liqun Chen Hewlett-Packard Laboratories , "Identity-based Cryptography ", '06.

[9] Mike Scott Dublin City University , "Efficient Implementation of Cryptographic pairings".

[10] Soonhak Kwon Department of Mathematics, Sungkyunkwan University, Korea," Efficient Tate Pairing Computation for Supersingular Elliptic Curves over Binary Fields ".

[11] P. S. L. M. Barreto, H. Y. Kim, B. Lynn and M. Scott, "Efficient Algorithms forPairing-Based Cryptosystems," Proc. Advances in Cryptology -- Crypto'02, pp.354-368, 2002.

[12] Wenbo Mao, Principal Engineer HP Labs., Bristol "Divisors, Bilinear Pairings and Pairing Enabled Cryptographic Applications".

[13] Paulo S. L. M. Barreto[1] , Alexandre Machado Deusajute "Toward Effcient Certificateless Signcryption from (and without) Bilinear Pairings".

[14] Wei Ren, Yoohwan Kim[1], Ju-Yeon Jo[2], Mei Yang[3] and Yingtao Jiang." IdSRF: ID- based Secure Routing Framework for Wireless Ad-Hoc Networks".

[15] D. B. Johnson and D. A. Maltz: *Dynamic Source Routing in Ad Hoc Wireless Networks*, In Mobile Computing, Chapter 5, P153-181, Kluwer Academic Publishers, 1996.

[16] Y. Hu, A. Perrig, D.B. Johnson, Ariadne: A secure On-Demand Routing Protocol for Ad-hoc Networks, Mobicom2002, September 23–26, 2002, Atlanta, Georgia, USA.

DOI: 01.ijns.01.02.05